TECH HIVE
ADVISORY

CYBERSECURITY PLAYBOOK

FOR BUSINESSES

Authors

Femi Adeleye
Fopefoluwa Ibraheem
Joyce Unwaetor

Reviewed by

Abiodun Gaffar

Designed by

Adeyinka Adeyemo

1. Introduction

Purpose of this Playbook

This playbook provides practical guidance for organisations to build basic cybersecurity practices and respond effectively to security incidents. It outlines simple steps businesses can take to reduce cyber risk, protect critical systems, and manage incidents when they occur.

Who This Playbook Is For

This document is intended for organisations of different sizes, including startups, small and medium-sized enterprises (SMEs), and larger organisations. It is also relevant for business leaders, IT teams, and operational staff responsible for managing organisational risk.

How to Use This Playbook

This playbook is designed as a practical guide. Organisations can use it as a starting point for building a cybersecurity framework, improving existing security practices, and guiding their response during cybersecurity incidents.

Cybersecurity as a Business Risk

Cybersecurity is not only a technical issue. Cyber incidents can disrupt operations, cause financial losses, and damage an organisation's reputation. For this reason, cybersecurity should be treated as a business risk that requires attention from leadership, staff, and technical teams.

2. Cybersecurity Governance and Ownership

Cybersecurity governance defines how an organisation directs, manages, and safeguards its digital systems, information assets, and operational technologies. In the modern digital environment, cybersecurity is no longer confined to technical specialists alone. Many cyber incidents originate from everyday organisational activities such as email communication, document sharing, remote work practices, and interactions with external partners. For this reason, effective cybersecurity governance recognises that security awareness and responsibility extend across the entire organisation, not solely within IT departments.

International best practices reflected in frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework developed by the National Institute of Standards and Technology emphasise that cybersecurity governance requires clear leadership responsibility, structured accountability, and organisation-wide awareness. In a well-governed cybersecurity environment, leadership provides direction, technical teams implement safeguards, and employees across all departments follow secure practices in their daily work.

Assigning cybersecurity responsibility (CISO, IT Lead, or Vendor)

Every organisation must formally designate a person or function responsible for coordinating cybersecurity strategy and overseeing security practices. This responsibility is typically assigned based on organisational size and operational complexity.

- **Chief Information Security Officer (CISO):** Large organisations commonly appoint a CISO responsible for cybersecurity strategy, policy development, risk management, and incident response coordination.
- **IT Lead or Technology Manager:** In smaller organisations, cybersecurity oversight may be handled by an IT manager or technology lead who manages both system operations and security controls.
- **Managed Security Service Providers (MSSPs):** Organisations may also engage specialised external vendors to provide services such as security monitoring, vulnerability assessment, and threat detection.

Regardless of the structure adopted, cybersecurity ownership must be clearly documented and embedded within organisational governance structures to ensure accountability and coordinated decision-making.

Creating cybersecurity policies

Cybersecurity policies provide the operational rules that guide how employees interact with organisational systems and information assets. These policies translate governance principles into practical instructions that staff can follow in their daily work.

Core cybersecurity policies typically address:

- Acceptable use of organisational devices and networks
- Access control and password management
- Data protection and information handling procedures
- Incident reporting and response protocols
- Third-party and vendor security practices
- Business continuity and disaster recovery measures

Policies must be formally approved, communicated clearly to employees, and supported through regular awareness and training programs. When staff understand the purpose and expectations of these policies, compliance becomes part of routine professional conduct.

Management oversight and reporting

Cybersecurity governance requires active oversight from senior leadership. Cyber risks can affect operational continuity, financial performance, and organisational reputation. As a result, cybersecurity must be integrated into enterprise risk management and leadership decision-making processes.

Organisations should establish structured reporting mechanisms that provide leadership with clear insight into cybersecurity performance and risks. Typical cybersecurity reports include:

- Security incident summaries
- Cyber risk assessments
- Compliance status with regulatory and industry standards
- Threat intelligence updates
- Performance evaluations of security controls

Regular reporting ensures that leadership maintains visibility over the organisation's security posture and can authorise timely improvements when necessary.

Cybersecurity budget planning

Effective cybersecurity programs require sustained financial investment. Budget planning must support both technological safeguards and organisational preparedness.

Cybersecurity expenditures commonly include:

- Security infrastructure and monitoring technologies
- Vulnerability testing and system audits
- Incident response capabilities
- Employee cybersecurity awareness training
- External security advisory or monitoring services

Organisations should adopt a risk-based budgeting approach, prioritising investments according to the potential impact of cyber threats on operations, data protection, and regulatory compliance.

3. Asset Management

A common challenge in cybersecurity is that organisations often do not have a complete picture of the technology they use. Devices are purchased, new applications are installed, teams sign up for online tools, and cloud infrastructure is created as the organisation grows. Over time, it becomes difficult to know exactly what systems exist and where organisational data is stored.

This creates risk. Systems that are not tracked are rarely monitored or maintained properly. They may miss security updates, use weak configurations, or store sensitive information without appropriate controls.

Asset management addresses this problem by ensuring the organisation maintains a clear inventory of its technology environment. This includes hardware devices, software applications, cloud services, and the data stored within those systems.

The goal is straightforward. The organisation should always be able to answer four basic questions:

- What devices are connected to our environment?
- What software are we running?
- What cloud services are we using?
- Where is our data stored?

Even for smaller organisations, maintaining this visibility makes it significantly easier to apply security controls and respond to potential incidents.

Hardware Asset Identification

Hardware assets include any physical device that connects to organisational systems or stores organisational data. These devices form the foundation of the technology environment and are often the first place security controls must be applied.

Common hardware assets include employee laptops, desktop computers, company issued mobile devices, servers, networking equipment such as routers and switches, and removable storage devices used for backups or file transfers.

The organisation should maintain a hardware inventory that records key details about each device. At a minimum this should include the device type, model, serial number, operating system, and the employee or team responsible for the device.

Field	Description
Asset ID	Unique identifier for the device
Device Type	Laptop, server, mobile device, etc.
Model / Manufacturer	Hardware details
Serial Number	Device serial number
Assigned User	Employee responsible for the device
Location	Office, remote, or data centre

Each device should have a clearly assigned owner. When devices are replaced, retired, or lost, the inventory should be updated.

For larger environments, endpoint management tools can automate much of this process by detecting devices and applying security policies.

Software, Application, and SaaS Asset Identification

Organisations rely on a wide range of applications to support daily operations. Some of these are installed directly on employee devices or internal servers, while others are delivered through cloud platforms as Software as a Service (SaaS). From a security perspective, both types introduce similar risks and therefore should be tracked in a consistent way.

Applications can store sensitive information, integrate with other systems, and provide access to critical business functions. If the organisation does not have visibility into which applications are being used, it becomes difficult to manage vulnerabilities, control access, or respond effectively to security incidents.

For this reason, the organisation should maintain a central inventory of all applications, regardless of whether they are installed locally or accessed through the cloud.

This inventory should include common business software such as productivity tools, development platforms, collaboration tools, financial systems, customer management platforms, and any internally developed applications. SaaS platforms such as Microsoft 365, Google Workspace, Slack, Salesforce, and similar services should also be included.

Maintaining a single application inventory helps the organisation understand which tools are being used across different teams and what role they play in daily operations.

It also makes it easier to monitor updates, manage licences, and identify applications that may no longer be required.

A practical application inventory may include the following information:

Field	Description
Application Name	Name of the software or service
Vendor / Provider	Organisation providing the application
Deployment Type	Installed software, internal system, or SaaS service
Version / Service Plan	Installed version or subscription tier
Business Owner	Team responsible for the application
Data Sensitivity	Type of organisational data stored or processed
Authentication Method	SSO, MFA, or local authentication
Approval Status	Approved, under review, or unauthorised

Where possible, organisations should define a list of approved applications. New tools should go through a simple review process before they are adopted widely. This helps ensure the organisation understands how the application works, what data it handles, and whether it meets security expectations.

Access to cloud based services should ideally be managed through a central identity provider using single sign on and multi factor authentication, particularly for systems that store sensitive data or provide administrative access.

Regular reviews of the application inventory can also help identify unused tools, duplicate services, or applications that are no longer supported. Maintaining visibility into the applications used across the organisation helps reduce security risk while ensuring teams can continue to work efficiently

Data Inventory and Classification

Data is often the most valuable asset an organisation holds. Understanding what data exists and where it is stored is essential for protecting it.

A data inventory identifies the types of information the organisation handles and the systems where that information is stored. This may include customer information, employee records, financial data, operational documents, and intellectual property.

Once identified, data should be classified based on its sensitivity.

Classification	Description
Public	Information intended for public release
Internal	Information used within the organisation
Confidential	Sensitive business or customer information
Restricted	Highly sensitive data requiring strict protection

Data classification helps guide how information should be handled. Sensitive data may require stronger access controls, encryption, or additional monitoring.

By understanding where data is stored and how sensitive it is, organisations can apply appropriate security measures and reduce the risk of accidental exposure.

4. Access Control and Identity Management

Access control ensures that only authorised individuals can access organisational systems and data. Many security incidents occur not because systems are technically breached, but because accounts have excessive permissions, weak authentication, or remain active after they should have been removed.

As organisations grow, employees, contractors, and partners may require access to different systems and applications.

Without clear controls, permissions can accumulate over time and increase the risk of accidental exposure or unauthorised access.

Effective identity and access management focuses on a few core practices. User accounts should be managed throughout their lifecycle, access should be limited to what users require for their role, and strong authentication should protect access to sensitive systems.

User Account Management

Each user should have a unique account linked to their identity. Shared accounts should be avoided wherever possible, as they reduce accountability and make activity difficult to trace.

User accounts should be created through a defined onboarding process and granted access based on the individual's role. When roles change, permissions should be reviewed and updated to reflect current responsibilities.

When employees or contractors leave the organisation, their access should be removed promptly. Periodic reviews of user accounts should also be conducted to identify inactive or unnecessary accounts.

Principle of Least Privilege

Users should only be granted the access required to perform their duties. This is known as the principle of least privilege.

Limiting permissions helps reduce the impact of both mistakes and compromised accounts. Most users do not require administrative privileges, and these permissions should be restricted to specific roles.

Where elevated access is required, it should be granted for a defined purpose and removed once the task is complete. Role-based access models can help organisations manage permissions consistently.

Multi-Factor Authentication (MFA)

Passwords alone are no longer sufficient to protect access to organisational systems. They can be guessed, reused, or exposed through phishing attacks and data breaches.

Multi factor authentication requires users to verify their identity using an additional factor, such as an authentication application or security key. This significantly reduces the likelihood of unauthorised access even if passwords are compromised.

MFA should be enabled for systems that store sensitive information or provide administrative access, including email platforms, cloud services, and remote access systems.

Password Policies

Strong password practices remain an important part of account security. Passwords should be long, unique, and difficult to guess.

Users should avoid reusing passwords across multiple services. A breach on one platform can otherwise expose credentials that provide access to organisational systems.

Password managers can help employees generate and store strong passwords securely while reducing the need to remember multiple complex credentials.

Privileged Access Management

Privileged accounts allow users to manage systems, change configurations, or access sensitive data. Because of the level of control they provide, these accounts are common targets for attackers.

Organisations should limit privileged access to a small number of authorised users and ensure it is granted only when necessary. Administrative accounts should be separate from standard user accounts used for daily work.

Where possible, actions performed using privileged accounts should be logged and monitored.

5. Endpoint and Device Security

Endpoints are the devices employees use to access organisational systems and data. These typically include laptops, desktops, and mobile devices. Because these devices interact directly with users and external networks, they are frequently targeted by attackers.

For many organisations, endpoints operate outside the office network for much of the time. Employees work from home, travel, and connect through different networks. This makes it important that each device is secured individually rather than relying only on network level protections.

Effective endpoint security focuses on protecting devices from malware, preventing unauthorised access, and ensuring systems remain properly maintained. Security controls such as endpoint protection software, encryption, and regular system updates help reduce the likelihood that compromised devices expose organisational data.

The practices described below help organisations strengthen the security of the devices that employees rely on every day.

Antivirus and Endpoint Detection and Response (EDR)

All organisational devices should run endpoint protection software capable of detecting malicious activity. Traditional antivirus tools identify known malware, while Endpoint Detection and Response solutions provide broader visibility into suspicious behaviour on a device.

EDR tools monitor system activity and can detect indicators such as unusual processes, unauthorised system changes, or attempts to access sensitive files. This allows potential threats to be identified and investigated earlier.

Endpoint protection software should be installed on all company managed devices and configured to receive regular updates. Alerts generated by these tools should be reviewed so that suspicious activity can be investigated in a timely manner.
Maintaining consistent endpoint protection across devices helps reduce the risk of malware infections and other endpoint based attacks.

Device Encryption

Devices often contain or provide access to sensitive organisational information. If a laptop or mobile device is lost or stolen, that data may be exposed unless the device is properly protected.

Device encryption helps address this risk by ensuring that data stored on the device cannot be accessed without proper authentication. Most modern operating systems provide built in encryption capabilities that can be enabled with minimal impact on users.

Organisations should require encryption for devices that store or access organisational data, particularly laptops and mobile devices used outside the office environment.

Encryption significantly reduces the risk of data exposure in the event that a device is lost, stolen, or otherwise accessed by unauthorised individuals.

Device Updates and Patch Management

Keeping devices updated is one of the most effective ways to prevent security incidents. Software vendors regularly release updates that address vulnerabilities discovered in operating systems and applications.

When devices are not updated, attackers may exploit known weaknesses that have already been patched elsewhere. For this reason, organisations should ensure that security updates are applied regularly across all managed devices.

Automatic updates can help ensure that patches are installed consistently. Organisations should also monitor device update status so that systems missing critical updates can be identified and addressed.
Consistent patch management helps reduce the likelihood that attackers exploit known vulnerabilities on endpoint devices.

Mobile Device Security

Mobile devices are commonly used to access email, collaboration platforms, and business applications. Because they are portable and frequently used outside controlled environments, they present unique security considerations.

Basic security controls should be applied to mobile devices that access organisational systems. These include device encryption, screen lock requirements, and the ability to remotely wipe organisational data if the device is lost or stolen.

Mobile device management tools can help organisations enforce these security settings and maintain visibility over mobile devices used for work purposes.
Applying these controls helps ensure that organisational data remains protected even when accessed from mobile devices.

Remote Work Security

Remote and hybrid work arrangements have become common across many organisations. While this offers flexibility, it also means that employees often connect to organisational systems from networks that are outside the organisation's direct control.

To reduce risk, remote access to organisational systems should be protected using secure authentication methods and encrypted connections. Multi factor authentication and secure access solutions help ensure that only authorised users can connect.

Employees should also follow basic security practices when working remotely, such as keeping devices updated, avoiding the use of shared or public computers, and connecting through trusted networks.
When endpoints are properly secured, organisations can support remote work while maintaining appropriate protection for their systems and data.

6. Network Security

The organisation's network forms the backbone of its digital operations. It connects user devices, internal systems, cloud services, and external partners. Because of this central role, the network is often a key target for attackers attempting to gain access to organisational systems or move laterally after an initial compromise.

Effective network security focuses on controlling how traffic enters and moves through the environment. This includes restricting unnecessary access, protecting wireless networks, limiting communication between systems, and maintaining visibility into network activity.

These controls help reduce the likelihood that unauthorised users gain access to the network and help contain potential incidents if a system becomes compromised.

Firewall Configuration

Firewalls should be used to control traffic entering and leaving the organisation's network. They provide a first layer of defence by filtering connections between internal systems and external networks.

Firewall rules should follow a default deny approach, where only required traffic is permitted. Services, ports, and protocols that are not needed for business operations should remain blocked.

Firewall configurations should also be reviewed periodically to ensure that rules remain appropriate and that temporary exceptions are removed when no longer required. Poorly maintained firewall rules can unintentionally expose internal systems to external access.

Secure Wi-Fi Setup

Wireless networks should be configured to prevent unauthorised access to the organisation's internal environment. Wi-Fi networks should use strong encryption and authentication mechanisms, and default router credentials should always be changed.

Where possible, organisations should maintain separate wireless networks for employees and visitors. Guest networks should provide internet access only and should not allow connections to internal systems or devices.

Limiting access to the wireless network reduces the risk of unauthorised users gaining a foothold within the organisation's environment.

Network Segmentation

Network segmentation helps reduce the impact of security incidents by limiting how systems communicate with one another.

In environments where all devices share a network, an attacker who compromises one system may be able to move freely across the environment. Segmentation helps contain this risk by separating systems into different network zones.

For example, user devices, servers, and sensitive systems can be placed on separate network segments with controlled communication. Even basic segmentation can significantly reduce the ability of attackers to move laterally within the network.

VPN Usage

Employees and administrators often need to access organisational systems from outside the office network. Virtual Private Networks provide a secure way to establish these connections.

VPN services encrypt traffic between the user and the organisation's network, helping protect sensitive information when accessing systems remotely.

Remote access should require strong authentication and should be limited to authorised users. Access permissions should also be reviewed periodically to ensure that only individuals who require remote access retain it.

Monitoring Network Activity

Maintaining visibility into network activity helps organisations detect suspicious behaviour and potential security incidents.

Network devices such as firewalls, routers, and monitoring systems can provide logs and alerts that indicate unusual traffic patterns, unexpected connections, or repeated authentication attempts.

Regularly reviewing network activity allows organisations to identify anomalies that may indicate compromise or misuse. Early detection is critical for limiting the impact of network based attacks.

7. Data Protection and Privacy

Data protection and privacy are essential components of a strong cybersecurity framework. organisations handle significant volumes of information every day, including customer records, employee data, financial information, and proprietary business documents. Protecting this data is necessary to maintain operational security, comply with regulatory requirements, and preserve the trust of customers and partners.

Global standards such as ISO/IEC 27001 and regulations like the General Data Protection Regulation emphasise the need for structured processes that govern how data is collected, stored, accessed, shared, and eventually deleted. A strong data protection strategy ensures that information remains secure throughout its entire lifecycle.

Data classification

Data classification is the process of organizing information based on its level of sensitivity and the level of protection it requires. When organisations clearly classify their data, they can apply the appropriate security controls and limit access to authorised individuals.

Organisations typically categorise data into the following groups:

- **Public data:** Information intended for public access and disclosure. This data carries minimal security restrictions.
- **Internal data:** Operational information meant for internal organisational use but not intended for public distribution.
- **Confidential data:** Sensitive information such as internal reports, business strategies, or operational documents that require controlled access.
- **Restricted or highly sensitive data:** Critical information such as financial records, personal data, intellectual property, or strategic documents that require the highest level of protection.

Once data is classified, organisations should apply corresponding access controls, storage protections, and monitoring measures.

Encryption (at rest and in transit)

Encryption protects information by converting it into coded data that can only be accessed with authorised decryption keys. This ensures that even if data is intercepted or accessed without permission, it cannot be read or misused.

Organisations should implement encryption in two primary contexts:

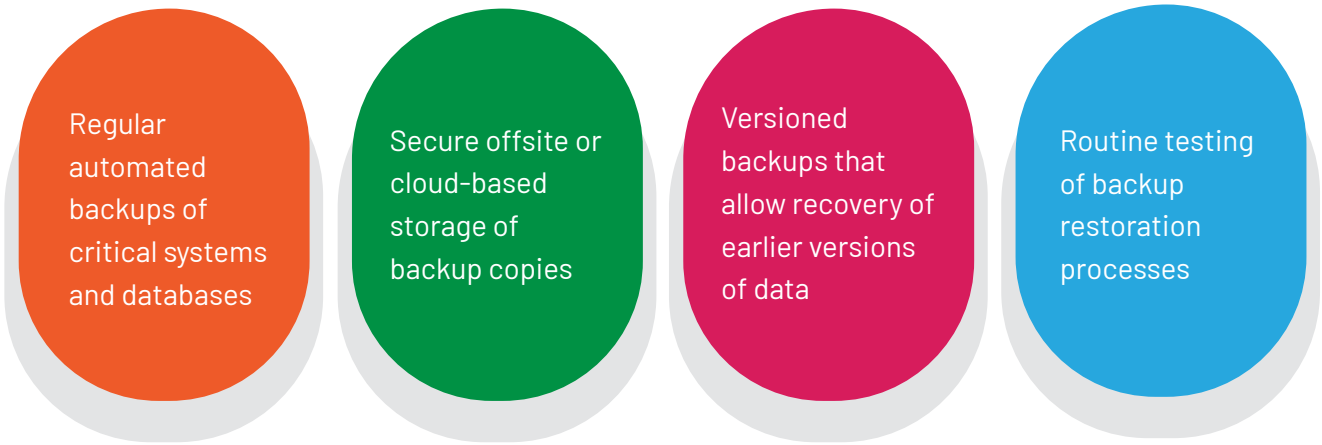
- **Data at rest:** Information stored in databases, servers, laptops, or cloud systems should be encrypted to prevent unauthorised access if systems are compromised or devices are lost.
- **Data in transit:** Information transmitted across networks such as emails, application communications, or file transfers, should be encrypted to prevent interception or unauthorised monitoring.

Encryption significantly reduces the risk of data exposure during both storage and communication.

Backup strategy

Data loss can occur due to cyberattacks, system failures, accidental deletion, or natural disasters. A structured backup strategy ensures that organisations can restore critical information and continue operations with minimal disruption.

An effective backup strategy should include:

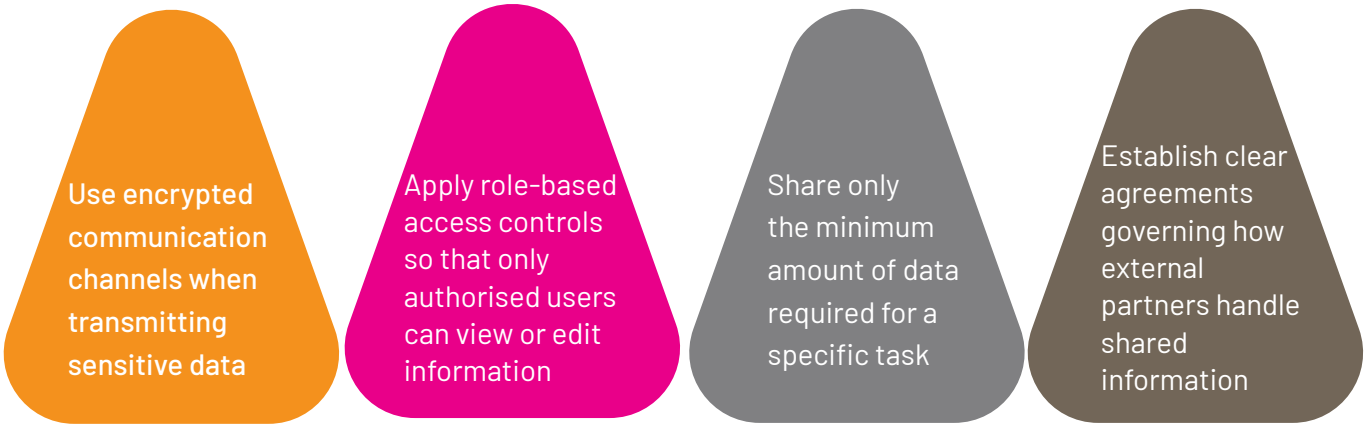


Testing recovery procedures is particularly important because it confirms that backups can actually be restored during an emergency.

Routine testing of backup restoration processes

Organisations frequently share information with employees, contractors, partners, and clients. Without proper safeguards, these exchanges can expose sensitive information to unauthorised access.

To ensure secure data sharing, organisations should:



These measures reduce the risk of accidental disclosure and strengthen overall data protection.

Data retention and deletion

Responsible data management requires organisations to retain information only for as long as it is necessary to meet operational, legal, or regulatory requirements. Storing unnecessary data increases exposure during a security incident.

Organisations should implement clear retention policies that define:

- The categories of data collected and stored
- The length of time each category should be retained
- The procedures used to securely delete or anonymise data once retention periods expire

Secure deletion ensures that sensitive information cannot be recovered once it is removed from active systems.

8. Email and Communication Security

Email remains one of the most common entry points for cyber attacks. Threat actors often use deceptive messages, malicious attachments, or fake links to gain access to organisational systems or sensitive information. For this reason, organisations should implement basic controls that reduce the risk of email-based attacks and protect internal communications.

Phishing Protection

Phishing attacks attempt to trick employees into revealing sensitive information or clicking malicious links. Organisations should train staff to recognise suspicious messages, verify unexpected requests, and report potential phishing attempts. Basic awareness training and regular reminders can significantly reduce the likelihood of successful phishing attacks.

Email Filtering

Email filtering tools help detect and block suspicious emails before they reach employees. These tools can scan incoming messages for malicious attachments, unsafe links, and known spam patterns. Implementing reliable email filtering reduces the risk of malware infections and fraudulent communications entering the organisation's network.

Secure Communication Tools

Sensitive business information should be shared through secure communication platforms that provide encryption and controlled access. Organisations should avoid sharing confidential information through unsecured channels and ensure that approved communication tools are used consistently across teams.

Email Authentication (SPF, DKIM, DMARC)

Email authentication mechanisms help prevent attackers from sending messages that appear to come from a legitimate organisational domain.

- SPF (Sender Policy Framework) verifies which mail servers are authorised to send emails on behalf of a domain.
- DKIM (DomainKeys Identified Mail) adds a digital signature to verify that an email has not been altered during transmission.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) builds on SPF and DKIM to help organisations monitor and enforce email authentication policies.

When implemented together, these controls reduce the risk of email spoofing and improve the organisation's ability to detect fraudulent messages.

9. Cloud Security

Cloud platforms now host many of the systems organisations depend on, including applications, data storage, and collaboration tools. While cloud providers secure the underlying infrastructure, organisations remain responsible for how their services are configured, accessed, and monitored.

Cloud environments can change quickly. New resources can be deployed in minutes, permissions can expand over time, and storage systems may unintentionally become accessible to the public internet. These issues often arise from misconfiguration rather than deliberate attack.

Managing cloud security therefore requires clear control over how services are configured, who can access them, how data is protected, and how activity is monitored. Establishing these practices helps reduce the risk of accidental exposure and ensures that security teams maintain visibility over the organisation's cloud environment.

Secure Configuration of Cloud Platforms

Cloud services should be deployed using secure configuration standards rather than relying on default settings. Many security incidents in cloud environments occur when storage systems, databases, or management interfaces are exposed unintentionally.

When new cloud resources are created, configurations should be reviewed to ensure that only required services are enabled and that public access is restricted unless explicitly needed. Administrative interfaces should also be protected from unnecessary external exposure.

Security capabilities provided by the cloud platform, such as encryption, logging, and security alerts, should be enabled as part of the initial configuration. Applying consistent configuration practices helps prevent common misconfigurations and ensures that cloud resources are deployed in a controlled and secure manner.

Access Controls for Cloud Services

Access management is one of the most important aspects of cloud security. Cloud platforms often provide broad permissions that can allow users to modify infrastructure, access data, or create new services.

Access should therefore follow the principle of least privilege. Users should only receive the permissions necessary to perform their responsibilities. Administrative privileges should be restricted to authorised personnel and used only when required.

Individual user identities should be used instead of shared accounts so that actions within the environment can be traced to specific users. Where possible, organisations should integrate cloud services with a central identity provider and enforce multi factor authentication, particularly for administrative roles.

Careful control of permissions helps prevent accidental changes and reduces the impact of compromised accounts.

Backup and Recovery

Although cloud services are designed to be resilient, they do not eliminate the risk of data loss. Files may be deleted accidentally, systems may be misconfigured, or malicious activity may disrupt services.

Organisations should ensure that critical systems and data stored in the cloud are backed up regularly. Backup processes should be designed so that data can be restored even if the primary environment becomes unavailable or compromised.

Recovery procedures should also be tested periodically. Verifying that backups can be restored successfully helps ensure that the organisation can recover quickly from data loss or service disruption.
Reliable backup and recovery capabilities are essential for maintaining operational continuity in cloud environments.

Monitoring Cloud Activity

Maintaining visibility into cloud activity is essential for detecting potential security issues. Cloud platforms generate logs that record actions such as user logins, configuration changes, and access to data.

Monitoring these logs helps organisations identify unusual behaviour that may indicate compromised accounts, unauthorised configuration changes, or other suspicious activity.

Security alerts and monitoring tools provided by cloud platforms should be enabled so that potential issues can be identified and investigated promptly. Logging also provides valuable information during incident investigations by showing how systems were accessed and what actions were taken.

Consistent monitoring helps ensure that organisations maintain awareness of activity within their cloud environments and can respond quickly when risks arise.

10. Employee Awareness and Training

Employees play an important role in maintaining an organisation's cybersecurity posture. Many cyber incidents begin with human error, such as clicking a malicious link or using weak passwords. Regular awareness and training help staff recognise threats and follow safe security practices.

Cybersecurity Awareness Programme

Organisations should establish a cybersecurity awareness programme that educates employees about common threats and safe online behaviour. Training should cover topics such as phishing, password security, safe internet use, and handling sensitive information. Awareness sessions can be delivered through workshops, short online courses, or internal security briefings.

Phishing Simulations

Organisations should establish a cybersecurity awareness programme that educates employees about common threats and safe online behaviour. Training should cover topics such as phishing, password security, safe internet use, and handling sensitive information. Awareness sessions can be delivered through workshops, short online courses, or internal security briefings.

Secure Password Practices

Employees should be encouraged to use strong and unique passwords for work accounts. Organisations may require minimum password length, the use of passphrases, and the use of password management tools where appropriate. Enabling multi-factor authentication can further reduce the risk of unauthorised access if passwords are compromised.

Reporting Suspicious Activity

Employees should know how and where to report suspicious emails, unusual system behaviour, or potential security incidents. Clear reporting channels, such as a dedicated security email address or internal reporting system, allow organisations to respond quickly to potential threats. Encouraging early reporting can help limit the impact of cyber incidents.

11. Vendor and Third-Party Risk Management

Most organisations do not operate alone. They rely on software providers, cloud platforms, consultants, managed service providers, and other external partners to deliver essential services. These relationships allow organisations to move faster and access specialised expertise.

However, every third-party connection also introduces risk.

A vendor may process organisational data, integrate with internal systems, or require administrative access to resolve technical issues. If the vendor's security practices are weak, the risk does not remain isolated to them. It can quickly become the organisation's problem as well.

Several high-profile breaches in recent years have originated through trusted vendors rather than direct attacks on the organisation itself. For this reason, organisations need a clear understanding of who their vendors are, what access they have, and how security responsibilities are shared.

Managing vendor risk does not require complex processes, but it does require visibility, clear expectations, and regular oversight.

Assessing Vendor Security Posture

Before working with a vendor that will store organisational data or integrate with internal systems, it is important to understand how that vendor approaches security.

This does not always require a detailed technical audit. In many cases, organisations can begin by reviewing basic security practices such as how the vendor protects data, manages user access, and responds to security incidents.

Documentation such as security policies, compliance certifications, or responses to security questionnaires can provide useful insight. The depth of this assessment should reflect the level of access the vendor will receive and the sensitivity of the data involved.

The goal is not to eliminate all risk, which is rarely possible, but to ensure that the organisation is working with vendors that take security seriously and can demonstrate appropriate safeguards.

Data Sharing Agreements

When organisational data is shared with a vendor, expectations around how that data will be used and protected should be clearly defined.

Data sharing or processing agreements help establish these expectations. They typically describe what information will be shared, why it is required, and what security measures the vendor must maintain when handling it.

These agreements may also define how long data can be retained, how incidents must be reported, and what happens to the data if the business relationship ends.

Clear agreements reduce ambiguity and help ensure that sensitive information is handled responsibly throughout the partnership.

Vendor Access Controls

Some vendors require access to internal systems in order to provide support, maintain infrastructure, or integrate services. When this access is granted, it should be carefully controlled.

Vendor accounts should follow the same standards applied to internal users.

Access should be linked to individual identities where possible and restricted to only the systems required for the vendor's work.

Temporary access is often appropriate for maintenance or troubleshooting tasks, and access should be removed once the work is complete. Multi-factor authentication should also be required for vendors accessing sensitive systems.

Controlling vendor access reduces the risk that external partners unintentionally introduce vulnerabilities into the organisation's environment.

Ongoing Monitoring

Vendor risk management should not stop once a contract is signed. Relationships evolve, services change, and new risks may emerge over time.

Organisations should periodically review which vendors have access to systems or data and confirm that this access remains necessary. Security incidents affecting a vendor or significant changes to the services they provide may also require reassessment.

Maintaining awareness of vendor relationships helps ensure that external partners continue to meet the organisation's security expectations. Consistent oversight helps organisations benefit from vendor partnerships while keeping associated risks under control.

12. Incident Response Plan

An incident response plan helps organisations respond quickly and effectively when a cybersecurity incident occurs. A structured response reduces confusion, limits damage, and supports faster recovery of affected systems and services.

How to Detect Incidents

Cybersecurity incidents can be identified through system alerts, unusual network activity, failed login attempts, or reports from employees. Organisations should monitor their systems regularly and ensure that staff understand how to recognise signs of suspicious activity, such as unexpected system behaviour, unauthorised access attempts, or unusual data transfers.

Incident Reporting Process

A clear reporting process allows employees to escalate potential security incidents quickly. Staff should report suspicious activity to the appropriate internal contact, such as the Cybersecurity team, as soon as it is detected. The reporting process should include basic details such as the time of the incident, the system affected, and a description of what was observed.

Incident Response Team Roles

Organisations should assign specific roles and responsibilities for responding to cybersecurity incidents. The incident response team may include IT personnel, security specialists, management representatives, and communication staff. Clearly defined roles help ensure that incidents are investigated, contained, and managed in a coordinated manner.

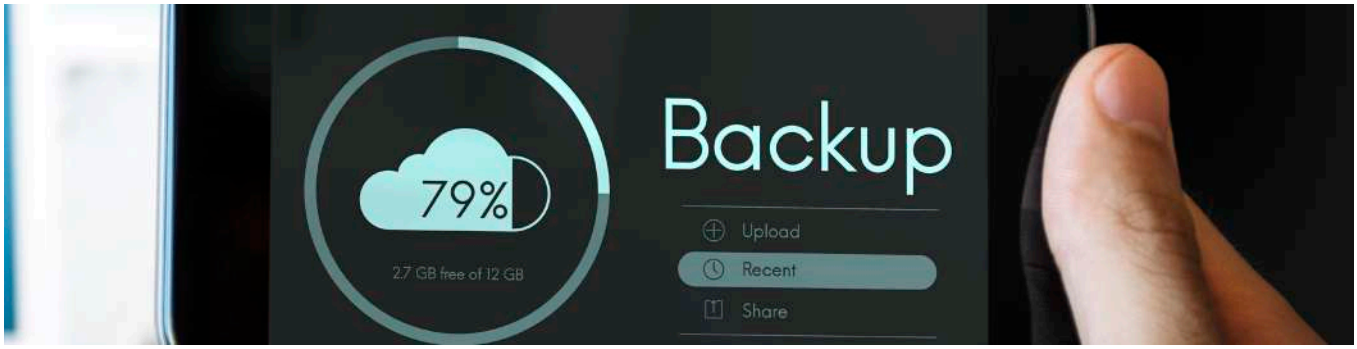
Containment and Recovery

Once an incident is confirmed, the organisation should take steps to contain the threat and prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious network activity. After containment, recovery actions may include restoring systems from backups, applying security patches, and verifying that systems are functioning normally.

Communication Plan

During a cybersecurity incident, clear communication is essential. Organisations should establish procedures for communicating with internal teams, management, and external stakeholders when necessary. This may include notifying customers, partners, or regulatory authorities depending on the nature and impact of the incident. Timely and accurate communication helps maintain trust and supports effective incident management.

13. Backup and Disaster Recovery



Backups and disaster recovery measures help organisations restore systems and data after a cyber incident, system failure, or other disruption. Regular backups and tested recovery procedures ensure that business operations can continue with minimal data loss.

Backup Frequency

Organisations should perform regular backups of critical data, systems, and applications. The frequency of backups depends on how often data changes and how important the information is to business operations. Many organisations schedule daily or weekly backups for essential systems to reduce the risk of significant data loss.

Backup Storage Security

Backups should be stored securely to prevent unauthorised access or tampering. Organisations may use encrypted storage and restrict access to authorised personnel only. It is also recommended to store backups in separate locations, such as secure off-site storage or cloud-based backup services, to protect data in case of physical damage or cyber attacks.

Recovery Testing

Backup systems should regularly be tested to ensure that data can be restored successfully when needed. Recovery testing allows organisations to confirm that backup files are complete, accessible, and capable of restoring systems within an acceptable time frame.

Business Continuity Planning

A business continuity plan outlines how an organisation will continue essential operations during and after a major disruption. This plan identifies critical systems, defines recovery priorities, and establishes procedures for restoring services as quickly as possible.

14. Monitoring and Continuous Improvement

Security controls are only effective if they are actively monitored and reviewed over time. Systems evolve, new technologies are introduced, and vulnerabilities are discovered regularly. Without continuous oversight, weaknesses can remain unnoticed until they are exploited.

Monitoring and periodic security assessments help organisations maintain visibility across their environment and identify issues before they develop into incidents. These activities provide insight into how systems are being used, where vulnerabilities exist, and whether existing security controls remain effective.

By regularly observing system activity, testing defences, and reviewing security practices, organisations can strengthen their overall security posture and respond more effectively to emerging risks.

Log Monitoring

Logs provide an important record of activity across systems, applications, and network infrastructure. They can capture events such as user logins, configuration changes, access to sensitive resources, and system errors.

Reviewing these logs helps organisations detect unusual or suspicious behaviour. Examples may include repeated failed login attempts, unexpected administrative activity, or access to systems outside normal usage patterns.

Organisations should enable logging for critical systems and ensure that logs are stored and retained appropriately. Where possible, monitoring tools can be used to highlight unusual activity and alert administrators to potential issues.
Maintaining visibility through log monitoring helps organisations detect and investigate security events more quickly.

Vulnerability Scanning

Vulnerability scanning helps organisations identify weaknesses in systems and applications that could be exploited by attackers. These scans look for known security issues such as missing patches, outdated software, or insecure configurations.

Regular vulnerability scanning allows organisations to maintain awareness of potential security gaps across their environment. Identified issues can then be prioritised and addressed based on their severity and potential impact.

Automated scanning tools can help simplify this process and provide continuous visibility into the organisation's security posture.

Penetration Testing

Penetration testing involves simulating real-world attacks to evaluate how effectively systems and security controls withstand exploitation attempts.

Security professionals performing a penetration test attempt to identify and exploit vulnerabilities in order to understand how an attacker might gain access to systems or sensitive data.

The results help organisations identify weaknesses that may not be visible through automated scanning and provide practical insight into how defences perform in realistic scenarios.
Penetration testing is particularly valuable for internet-facing systems, critical applications, or after significant infrastructure changes.

Security Audits

Security audits provide a structured review of the organisation's security controls, policies, and operational practices. These reviews help confirm that security measures are implemented consistently and functioning as intended.

Audits may evaluate areas such as system configurations, access controls, policy compliance, and data protection practices.

By periodically reviewing these areas, organisations can identify gaps in implementation and ensure that security practices remain aligned with organisational requirements and regulatory obligations.

Continuous Improvement

Security monitoring and assessments provide valuable insight into how well an organisation's security measures are performing. Findings from logs, vulnerability scans, penetration tests, and audits should be used to inform ongoing improvements.

Organisations should periodically review these findings, address identified weaknesses, and update security practices where necessary.

A structured approach to continuous improvement helps ensure that security measures evolve alongside the organisation's systems, technologies, and risk environment.

15. Legal, Compliance, and Regulatory Requirements

Organisations operating in the digital environment must ensure that their cybersecurity practices align with applicable legal, regulatory, and industry requirements. Cybersecurity failures can expose organisations not only to operational disruptions but also to legal liability, regulatory sanctions, financial penalties, and reputational damage. For this reason, compliance with established legal frameworks and industry standards forms an essential component of any cybersecurity program.

Effective compliance requires organisations to understand the legal obligations governing how they collect, process, store, and protect information. These obligations may arise from national laws, international regulations, contractual commitments, or industry-specific requirements. A structured compliance approach ensures that cybersecurity practices remain aligned with legal expectations and recognised global standards.

Applicable laws and regulations

Organisations must identify and comply with the laws and regulations that govern their operations, particularly those relating to information security, data protection, consumer protection, and digital services. The specific legal requirements may vary depending on the jurisdiction in which the organization operates and the sectors in which it conducts business.

Examples of widely recognised regulatory frameworks include:

- General Data Protection Regulation, which establishes comprehensive requirements for protecting personal data within the European Union and for organisations that process data of EU residents.
- Nigeria Data Protection Act, which regulates the processing and protection of personal data within Nigeria.
- Sector-specific regulations governing financial institutions, telecommunications operators, healthcare organisations, and other critical service providers.

Organisations must periodically review the legal frameworks applicable to their operations and ensure that their cybersecurity policies and operational procedures remain compliant with these obligations.

Data protection obligations

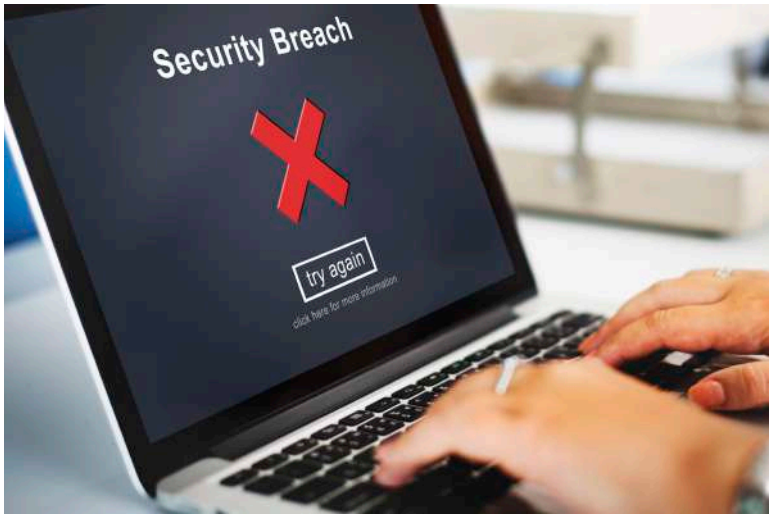
Legal and regulatory frameworks typically impose specific responsibilities on organisations that collect or process personal data. These obligations require organisations to implement appropriate technical and organisational safeguards to protect individuals' information from unauthorised access, disclosure, alteration, or loss.

Common data protection obligations include:

- Collecting personal data only for legitimate and clearly defined purposes
- Ensuring that data processing activities are lawful, transparent, and proportionate
- Implementing security measures to protect personal data from breaches or unauthorised access
- Limiting access to personal data to authorised personnel only
- Providing mechanisms for individuals to exercise their data protection rights where applicable

Compliance with these obligations strengthens public trust and ensures responsible handling of personal and sensitive information.

Breach notification requirements



Many legal frameworks require organisations to report data breaches or cybersecurity incidents that may compromise personal or sensitive information. Timely breach notification allows affected individuals, regulators, and stakeholders to take appropriate protective measures.

Organisations should establish clear procedures for identifying, documenting, and reporting security incidents. These procedures should include:

- Internal processes for detecting and assessing potential data breaches
- Clear reporting channels for employees to escalate suspected incidents
- Defined timelines for notifying regulatory authorities when required by law
- Communication protocols for informing affected individuals where appropriate

Prompt reporting and transparent communication are essential components of responsible cybersecurity governance and regulatory compliance.

Industry standards (ISO 27001, NIST, etc.)

In addition to legal requirements, organisations are encouraged to adopt internationally recognised cybersecurity standards that provide structured guidance for managing information security risks. These standards support the consistent implementation of security controls and strengthen overall governance frameworks.

Widely adopted standards include:

- **ISO/IEC 27001:** A globally recognised framework for establishing, implementing, maintaining, and continually improving an information security management system.
- **NIST Cybersecurity Framework developed by the National Institute of Standards and Technology:** structured framework that guides organisations in identifying, protecting against, detecting, responding to, and recovering from cybersecurity threats.

Adopting these standards helps organisations align their cybersecurity practices with international best practices while strengthening operational resilience.

16. Cybersecurity Maturity Self-Assessment

A cybersecurity maturity self assessment helps organisations evaluate the strength of their cybersecurity practices and identify areas that require improvement. Cybersecurity maturity reflects how well an organization can prevent, detect, respond to, and recover from cyber threats. Rather than assuming that security controls are effective, a structured assessment allows organisations to measure their current posture against recognised frameworks and best practices.

Frameworks such as NIST Cybersecurity Framework developed by the National Institute of Standards and Technology and ISO/IEC 27001 encourage organisations to periodically assess their security maturity and strengthen controls as digital risks evolve.

The following checklist provides a simplified maturity model that organisations can use to evaluate their cybersecurity readiness across three levels.

Basic Level Checklist

Organisations at the basic maturity level have implemented foundational cybersecurity practices. These controls provide initial protection against common cyber threats but may not yet include comprehensive monitoring or formalised security governance.

Indicators of basic cybersecurity maturity include:

- Basic antivirus and endpoint protection installed on organisational devices
- Strong password requirements and basic access controls implemented
- Regular software and system updates performed
- Basic data backups conducted periodically
- Employees receive introductory cybersecurity awareness guidance
- Use of secure Wi Fi networks and device protection measures
- Clear reporting channel for suspicious emails or digital activity

Organisations operating at this level should prioritise establishing structured policies, improving employee awareness, and implementing stronger monitoring capabilities.

Intermediate Level Checklist

Organisations at the intermediate maturity level have implemented more structured cybersecurity governance and operational controls. Security processes are documented and integrated into routine business activities.

Indicators of intermediate cybersecurity maturity include:

- Documented cybersecurity policies and procedures
- Role based access control implemented across key systems
- Multi factor authentication used for sensitive systems or accounts
- Regular vulnerability assessments and system monitoring conducted
- Formal data classification and data protection practices established
- Role based access control implemented across key systems
- Incident response procedures documented and communicated to staff
- Cybersecurity awareness training is regularly conducted across departments

At this stage, organisations move beyond basic protection and begin developing proactive mechanisms for identifying and responding to security risks.

Advanced Level Checklist

Organisations at the advanced maturity level maintain a comprehensive cybersecurity program supported by strong governance, continuous monitoring, and strategic risk management.

Indicators of advanced cybersecurity maturity include:

- Dedicated cybersecurity leadership such as a Chief Information Security Officer or equivalent role
- Formal vendor and third party cybersecurity risk management processes implemented
- Continuous monitoring systems and threat detection technologies in place
- Incident response teams trained and capable of coordinated response actions
- Regular penetration testing and independent security audits conducted
- Cybersecurity metrics regularly reported to executive leadership
- Security integrated into enterprise risk management and strategic planning
- Compliance with international standards such as ISO/IEC 27001

Organisations operating at this level demonstrate strong resilience against cyber threats and continuously refine their security capabilities.

Risk Scoring

To support objective evaluation, organisations can apply a simple scoring system to the maturity assessment. Each checklist item can be rated based on the organization's level of implementation.

Suggested scoring approach:

0 points if the control is not implemented

1 point if the control is partially implemented

2 points if the control is fully implemented

After completing the checklist, organisations can calculate their maturity score and interpret the results as follows:

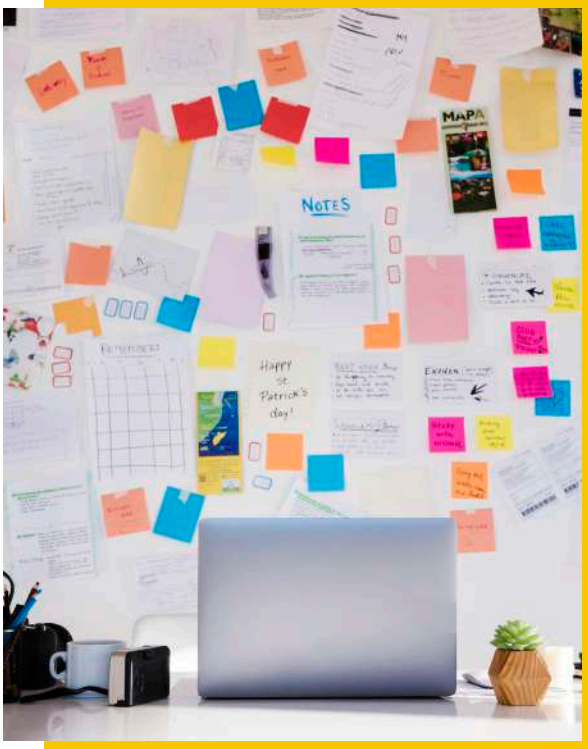
Low maturity: Security practices are limited and require immediate improvement.

Moderate maturity: Core cybersecurity practices are established but require strengthening and expansion.

High maturity: Security controls are comprehensive and integrated into organisational governance.

Regular reassessment helps organisations monitor progress and ensure that cybersecurity capabilities evolve alongside technological changes and emerging threats.

17. Templates and Resources



Templates and practical resources support the consistent implementation of cybersecurity practices across an organization. While policies and frameworks provide strategic guidance, operational templates help teams document activities, track risks, and maintain accountability in day to day security management.

Organisations that maintain standardised templates improve record keeping, strengthen compliance practices, and ensure that security procedures are applied consistently across departments. These resources also support internal reviews, audits, and regulatory reporting where required.

The following templates provide practical tools that organisations can adopt as part of their cybersecurity playbook.

Incident report template

An incident report template provides a structured format for documenting cybersecurity incidents, including suspected breaches, system disruptions, or unauthorised access attempts. Proper documentation supports investigation, response coordination, and compliance with reporting obligations.

A standard incident report template should include:

- **Incident identification number:** Unique reference number for tracking the incident.
- **Date and time of detection:** When the incident was first identified.
- **Reporter information:** Name and department of the person reporting the incident.
- **Description of the incident:** Clear summary of what occurred and how the incident was discovered.
- **Affected systems or data:** Systems, networks, or information potentially impacted.
- **Immediate actions taken:** Steps taken to contain or mitigate the incident.
- **Impact assessment:** Initial evaluation of operational, financial, or data related impacts.
- **Escalation and response actions:** Actions taken by the cybersecurity or IT response team.
- **Resolution and follow up measures:** Final outcome and recommended preventive actions.

Maintaining consistent incident documentation strengthens an organization's ability to analyse patterns and improve future response strategies.

Asset register template

An asset register provides a comprehensive record of the organisation's digital and technological resources. Maintaining an updated inventory of assets helps organisations understand what systems require protection and where potential vulnerabilities may exist.

A cybersecurity asset register should capture:

- **Asset name and description:** Identification of the system, device, or software.
- **Asset owner or responsible department:** Individual or team responsible for the asset.
- **Location or hosting environment:** Physical location or cloud environment where the asset is stored.
- **Asset classification level:** Sensitivity level based on the organization's data classification framework.
- **System purpose or function:** Operational role of the asset.
- **Security controls applied:** Existing protections such as encryption, authentication, or monitoring.
- **Last review or update date:** Date of the most recent asset verification.

Maintaining a comprehensive asset register supports risk management and enables organisations to prioritise security protections effectively.

Access control template

An access control template helps organisations document and manage user permissions across systems, applications, and data repositories. Proper access management ensures that employees can only access the information required to perform their work responsibilities.

An access control record should include:

- **User name and role:** Identification of the employee or system user.
- **Department or business unit:** organisational unit associated with the user.
- **System or application accessed:** Specific platform, database, or service.
- **Access level granted:** Permission level such as read only, edit, or administrative access.
- **Approval authority:** Manager or system administrator who authorised the access.
- **Access start date:** Date access was granted.
- **Review or expiration date:** Date when access should be reviewed or revoked.

Regular review of access control records helps prevent unauthorised access and reduces the risk of internal security incidents.

Vendor assessment template

Third party vendors often require access to organisational systems or data. A vendor assessment template allows organisations to evaluate the cybersecurity practices of external partners before granting system access or sharing sensitive information.

A vendor cybersecurity assessment should evaluate:

- **Vendor organization details:** Name, contact information, and service provided.
- **Type of data accessed or processed:** Nature and sensitivity of information handled by the vendor.
- **Security certifications or standards followed:** Compliance with standards such as ISO/IEC 27001.
- **Data protection measures implemented:** Encryption, access controls, and monitoring practices.
- **Incident response procedures:** Vendor capability to detect and respond to security incidents.
- **Data sharing and storage practices:** Where and how the vendor stores or processes data.
- **Contractual security obligations:** Security commitments defined within service agreements.

Conducting vendor assessments helps organisations reduce risks associated with third party access to critical systems and information.

Policy templates

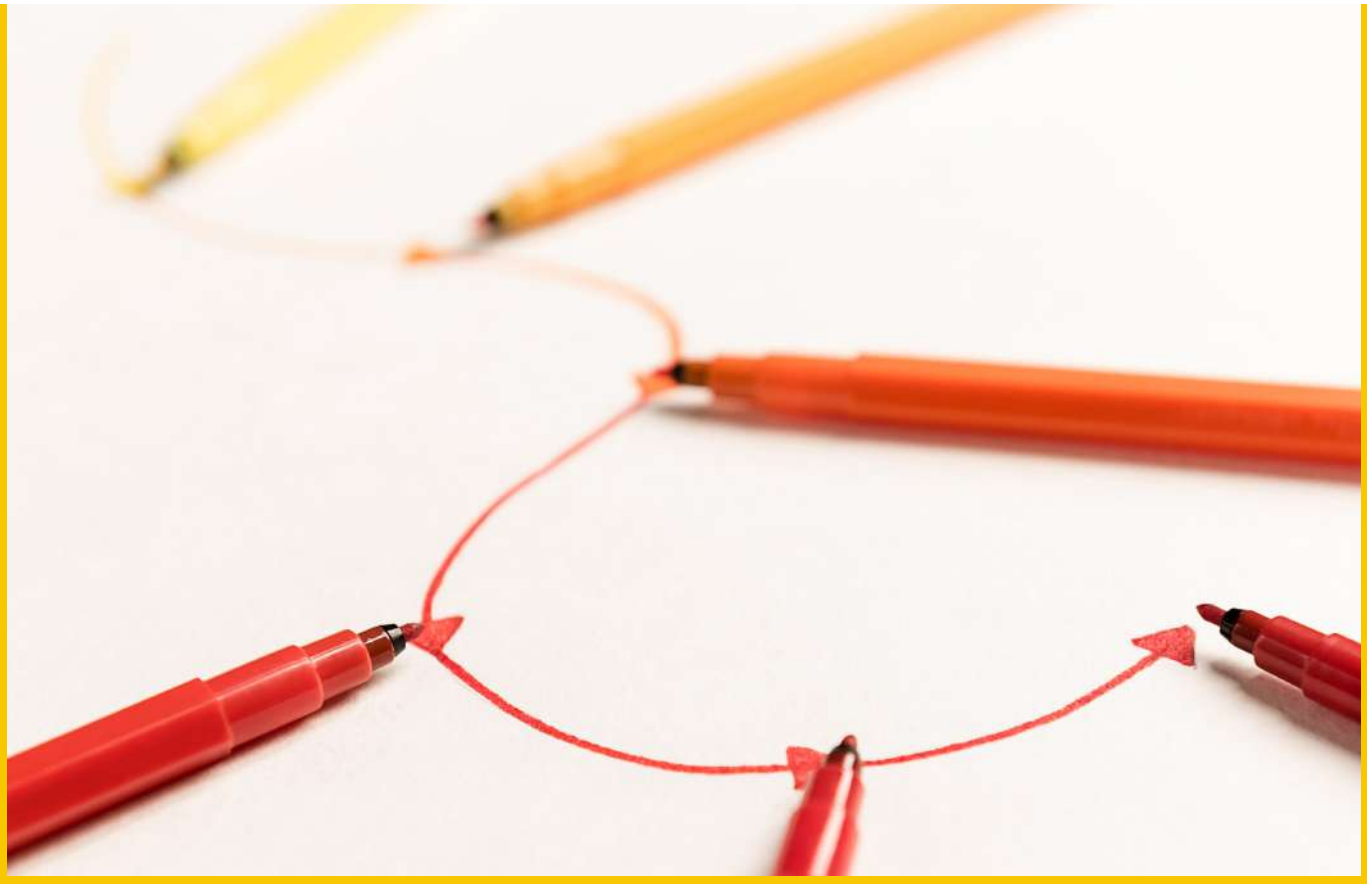
Policy templates provide organisations with a standardised structure for developing formal cybersecurity policies. These templates ensure that policies remain consistent, comprehensive, and aligned with recognised security frameworks.

Common policy templates include:

- **Information security policy:** Defines the organisation's overall cybersecurity objectives and governance structure.
- **Acceptable use policy:** Outlines rules for employee use of organisational devices, networks, and digital resources.
- **Access control policy:** Establishes procedures for granting, managing, and revoking system access.
- **Data protection policy:** Defines requirements for handling, storing, and protecting sensitive information.
- **Incident response policy:** Describes procedures for detecting, reporting, and responding to cybersecurity incidents.

Policy templates support faster policy development while ensuring that key security principles are consistently reflected in organisational procedures.

18. Action Plan and Implementation Roadmap



A cybersecurity playbook is most effective when supported by a clear implementation plan. An action plan and roadmap help organisations move from policy development to practical execution by identifying immediate priorities, medium term improvements, and long term strategic goals. A phased implementation approach allows organisations to strengthen their cybersecurity posture progressively while aligning security initiatives with operational capacity and available resources.

International best practices reflected in frameworks such as NIST Cybersecurity Framework developed by the National Institute of Standards and Technology and ISO/IEC 27001 recommend structured planning that integrates governance, risk management, and continuous improvement.

The following roadmap outlines practical priorities across three phases.

First 30 days priorities

The first phase focuses on establishing visibility into existing cybersecurity practices and implementing essential safeguards that address immediate risks.

Key actions during this period include:

Conduct an initial cybersecurity assessment:
Review current systems, policies, and controls to understand the organization's existing cybersecurity posture.

Identify and document critical digital assets:
Create an asset inventory that includes systems, devices, applications, and sensitive data repositories.

Assign cybersecurity responsibility:
Designate an internal security lead or responsible officer to coordinate cybersecurity efforts.

Review access controls:
Ensure that only authorised users have access to critical systems and remove unnecessary permissions.

Implement essential security updates:
Confirm that operating systems, applications, and network infrastructure are updated with the latest security patches.

Establish incident reporting procedures:
Create a clear internal process for reporting suspicious digital activity or potential security incidents

Introduce basic cybersecurity awareness guidance for employees:
Provide staff with essential guidance on password protection, phishing awareness, and secure system usage.

These early actions create the foundation for more structured cybersecurity improvements.

First 90 days priorities

The second phase focuses on strengthening governance structures, formalising policies, and implementing stronger technical and operational safeguards.

Key priorities during this stage include:

Develop and approve cybersecurity policies:
Establish formal policies covering data protection, access control, acceptable system use, and incident response.

Implement data protection practices:
Introduce data classification procedures, encryption safeguards, and structured data backup systems.

Strengthen authentication controls:
Implement multi factor authentication for sensitive systems and administrative accounts.

Conduct vulnerability assessments:
Evaluate systems for potential weaknesses and apply remediation measures.

Introduce cybersecurity training programs:
Provide employees with structured training that builds awareness of cyber risks and secure work practices.

Establish vendor cybersecurity assessment processes:
Evaluate third party service providers that access organisational systems or sensitive information.

Implement regular security monitoring procedures:
Establish processes for monitoring network activity and identifying suspicious behaviour.

This phase transitions the organisation from basic protection toward structured cybersecurity management.

First 90 days priorities

The long term phase focuses on building a mature cybersecurity program that is integrated into organisational governance and strategic planning.

Long term priorities include:

Establish a formal cybersecurity governance framework:
Integrate cybersecurity into enterprise risk management and executive oversight processes.

Implement continuous security monitoring and threat detection:
Adopt advanced monitoring tools that enable early detection of cyber threats.

Conduct regular penetration testing and independent security audits:
Assess the effectiveness of existing security controls and identify emerging vulnerabilities.

Align cybersecurity practices with international standards:
Adopt recognised frameworks such as ISO/IEC 27001.

Strengthen incident response and recovery capabilities:
Develop coordinated response procedures and conduct periodic response simulations.

Establish cybersecurity performance metrics and reporting:
Provide employees with structured training that builds awareness of cyber risks and secure work practices.

Promote a culture of cybersecurity awareness across the organisation:
Embed secure digital practices into everyday business operations.

Over time, these initiatives enable organisations to develop a resilient cybersecurity posture capable of adapting to evolving digital threats.

19. Implementation Support

This playbook provides practical guidance to help your organisation improve cybersecurity, but some organisations may benefit from additional support to implement these practices fully. We can assist with activities that strengthen your security posture, build internal capabilities, and ensure compliance with recognised standards.

Areas where we can provide support include:

a. **Team Training and Certifications:** Supporting IT and security teams in gaining recognised industry credentials.

b. **Cybersecurity Awareness Programmes:** Providing tailored training to improve employee awareness of cyber risks.

c. **Incident Response Management:** Assisting with the creation and testing of incident response plans and providing guidance during incidents.

e. **Risk Assessments and Vulnerability Testing:** Helping identify weaknesses, prioritise risks, and implement measures to reduce vulnerabilities.

d. **ISO/IEC 27001 Certification:** Helping organisations establish a structured information security management system and prepare for certification.

References

NIST Cybersecurity Framework (CSF) 2.0, https://www.nist.gov/cyberframework accessed 12 March 2026
National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity 18 March 2026.
Olzak T, Cybersecurity Risk Analysis and Management (2025) ResearchGate https://www.researchgate.net/publication/389652223_Cybersecurity_Risk_Analysis_and_Management accessed 12 March 2026
Weathering the Storm: Examining How Organisations Navigate the Sea of Cybersecurity Regulations' (2024) Information Systems Journal (Taylor & Francis) accessed 18 March 2026.
'Cybersecurity Framework' ScienceDirect Topics https://www.sciencedirect.com/topics/computer-science/cybersecurity-framework accessed 8 March 2026.
Oluwatosin Ilori, Nelly Tochi Nwosu and Henry Nwapali Ndidi Naiho, 'Third-Party Vendor Risks in IT Security: A Comprehensive Audit Review and Mitigation Strategies' (2024) World Journal of Advanced Research and Reviews 22 (3) 213 https://www.researchgate.net/publication/381844798_Third-Party_Vendor_Risks_in_IT_Security_A_Comprehensive_Audit_Review_and_Mitigation_Strategies accessed 6 March 2026.
Stefan Rass and others, Governing Cybersecurity from the Boardroom: Challenges, Drivers and Ways Ahead (2023) https://www.researchgate.net/publication/362144240_Governing_Cybersecurity_from_the_Boardroom_Challenges_Drivers_and_Ways_Ahead accessed 7 March 2026.

TECH HIVE
ADVISORY